
بسم الله الرحمن الرحيم

دانشگاه تربیت مدرّس

دانشکده مهندسی برق و کامپیوتر، گروه کامپیوتر

پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر- نرم افزار

تشخیص رفتار غیرعادی در شبکه‌های اقتضایی مبتنی بر پروتکل مسیریابی OLSR

حجت گهرگزی

استاد راهنما:

دکتر سعید جلیلی

استاد مشاور:

دکتر مهدی آبادی

آبان ۱۳۹۱

آیین‌نامه حق مالکیت مادی و معنوی در مورد نتایج پژوهشهای علمی دانشگاه تربیت مدرس

مقدمه: با عنایت به سیاست‌های پژوهشی و فناوری دانشگاه در راستای تحقق عدالت و کرامت انسانها که لازمه شکوفایی علمی و فنی است و رعایت حقوق مادی و معنوی دانشگاه و پژوهشگران، لازم است اعضای هیأت علمی، دانشجویان، دانش‌آموختگان و دیگر همکاران طرح، در مورد نتایج پژوهشهای علمی که تحت عناوین پایان‌نامه، رساله و طرحهای تحقیقاتی با هماهنگی دانشگاه انجام شده است، موارد زیر را رعایت نمایند:

ماده ۱- حق نشر و تکثیر پایان نامه/ رساله و درآمدهای حاصل از آنها متعلق به دانشگاه می باشد ولی حقوق معنوی پدید آورندگان محفوظ خواهد بود.

ماده ۲- انتشار مقاله یا مقالات مستخرج از پایان‌نامه/ رساله به صورت چاپ در نشریات علمی و یا ارائه در مجامع علمی باید به نام دانشگاه بوده و با تایید استاد راهنمای اصلی، یکی از اساتید راهنما، مشاور و یا دانشجو مسئول مکاتبات مقاله باشد. ولی مسئولیت علمی مقاله مستخرج از پایان نامه و رساله به عهده اساتید راهنما و دانشجو می باشد.

تبصره: در مقالاتی که پس از دانش‌آموختگی بصورت ترکیبی از اطلاعات جدید و نتایج حاصل از پایان‌نامه/ رساله نیز منتشر می‌شود نیز باید نام دانشگاه درج شود.

ماده ۳- انتشار کتاب، نرم افزار و یا آثار ویژه (اثری هنری مانند فیلم، عکس، نقاشی و نمایشنامه) حاصل از نتایج پایان‌نامه/ رساله و تمامی طرحهای تحقیقاتی کلیه واحدهای دانشگاه اعم از دانشکده ها، مراکز تحقیقاتی، پژوهشکده ها، پارک علم و فناوری و دیگر واحدها باید با مجوز کتبی صادره از معاونت پژوهشی دانشگاه و براساس آئین نامه های مصوب انجام شود.

ماده ۴- ثبت اختراع و تدوین دانش فنی و یا ارائه یافته ها در جشنواره‌های ملی، منطقه‌ای و بین‌المللی که حاصل نتایج مستخرج از پایان‌نامه/ رساله و تمامی طرح‌های تحقیقاتی دانشگاه باید با هماهنگی استاد راهنما یا مجری طرح از طریق معاونت پژوهشی دانشگاه انجام گیرد.

ماده ۵- این آیین‌نامه در ۵ ماده و یک تبصره در تاریخ۸۷/۴/۱ در شورای پژوهشی و در تاریخ ۸۷/۴/۲۳ در هیأت رئیسه دانشگاه به تایید رسید و در جلسه مورخ ۸۷/۷/۱۵ شورای دانشگاه به تصویب رسیده و از تاریخ تصویب در شورای دانشگاه لازم‌الاجرا است.

«اینجانب **حجت گهرگزی** دانشجوی رشته **مهندسی کامپیوتر- نرم افزار** ورودی سال تحصیلی **۹۰-۱۳۸۹** مقطع **کارشناسی ارشد** دانشکده **مهندسی برق و کامپیوتر** متعهد می شوم کلِیه نکات مندرج در آئین نامه حق مالکیت مادی و معنوی در مورد نتایج پژوهش های علمی دانشگاه تربیت مدرس را در انتشار یافته های علمی مستخرج از پایان نامه / رساله تحصیلی خود رعایت نمایم. در صورت تخلف از مفاد آئین نامه فوق الاشعار به دانشگاه وکالت و نمایندگی می دهم که از طرف اینجانب نسبت به لغو امتیاز اختراع بنام بنده و یا هر گونه امتیاز دیگر و تغییر آن به نام دانشگاه اقدام نماید. ضمناً نسبت به جبران فوری ضرر و زیان حاصله بر اساس برآورد دانشگاه اقدام خواهم نمود و بدینوسیله حق هر گونه اعتراض را از خود سلب نمودم»

امضا: حجت گهرگزی

تاریخ: ۹۱/۱۰/۲۴

آیین نامه چاپ پایان‌نامه (رساله)های دانشجویان دانشگاه تربیت مدرس

نظر به اینکه چاپ و انتشار پایان نامه (رساله)های تحصیلی دانشجویان دانشگاه تربیت مدرس، مبین بخشی از فعالیتهای علمی - پژوهشی دانشگاه است بنابراین به منظور آگاهی و رعایت حقوق دانشگاه،دانش آموختگان این دانشگاه نسبت به رعایت موارد ذیل متعهد می‌شوند:

ماده ۱: در صورت اقدام به چاپ پایان نامه (رساله)ی خود، مراتب را قبلاً به طور کتبی به «دفتر نشر آثارعلمی» دانشگاه اطلاع دهد.

ماده ۲: در صفحه سوم کتاب (پس از برگ شناسنامه) عبارت ذیل را چاپ کند:

«کتاب حاضر، حاصل پایان نامه کارشناسی ارشد/ رساله دکتری نگارنده در رشته مهندسی کامپیوتر- نرم افزار است که در سال ۱۳۹۱ در دانشکده مهندسی برق و کامپیوتر دانشگاه تربیت مدرس به راهنمایی جناب آقای دکتر سعید جلیلی، شاوره جناب آقای دکتر مهدی آبادی از آن دفاع شده است.»

ماده ۳: به منظور جبران بخشی از هزینه‌های انتشارات دانشگاه، تعداد یک درصد شمارگان کتاب (در هر نوبت‌چاپ) را به «دفتر نشر آثارعلمی» دانشگاه اهدا کند. دانشگاه می‌تواند مازاد نیاز خود را به نفع مرکز نشر درمعرض فروش قرار دهد.

ماده ۴: در صورت عدم رعایت ماده ۳، ۵۰٪ بهای شمارگان چاپ شده را به عنوان خسارت به دانشگاه تربیت‌مدرس، تأدیه کند.

ماده ۵: دانشجو تعهد و قبول می کند در صورت خودداری از پرداخت بهای خسارت، دانشگاه می‌تواند خسارت مذکور را از طریق مراجع قضایی مطالبه و وصول کند؛ به علاوه به دانشگاه حق می‌دهد به منظور استیفای حقوق خود، از طریق دادگاه، معادل وجه مذکور در ماده ۴ را از محل توقیف کتابهای عرضه شده نگارنده برای فروش، تامین نماید.

ماده ۶: اینجانب **حجت گهرگزی** دانشجوی رشته **مهندسی کامپیوتر- نرم افزار** مقطع **کارشناسی ارشد**

تعهد فوق وضمانت اجرایی آن را قبول کرده، به آن ملتزم می شوم.

نام و نام خانوادگی: حجت گهرگزی

تاریخ و امضا: ۹۱/۱۰/۲۴

دانشگاه تربیت مدرس
دانشکده مهندسی برق و کامپیوتر

بسمه تعالی

تاییدیه اعضای هیات داوران حاضر در جلسه دفاع از پایان نامه کارشناسی ارشد

آقای **حجت گهرگزی** پایان نامه ۶ واحدی خود را با عنوان **تشخیص رفتار غیر عادی در شبکه های بیسیم اقتضایی مبتنی بر پروتکل مسیر یابی** OLSR در تاریخ ۱۳۹۱/۸/۲۰ ارائه کردند.

اعضای هیات داوران نسخه نهایی این پایان نامه را از نظر فرم و محتوا تایید کرده، پذیرش آنرا برای اخذ درجه کارشناسی ارشد مهندسی کامپیوتر-نرم افزار پیشنهاد می کنند.

عضو هیات داوران	نام و نام خانوادگی	رتبه علمی	امضا
استاد راهنما	دکتر سعید جلیلی	دانشیار	
استاد مشاور	دکتر مهدی آبادی	استادیار	
استاد ناظر	دکتر محمد صنیعی آباده	استادیار	
استاد ناظر	دکتر سیاوش خرسندی	استادیار	
مدیر گروه (یا نماینده گروه تخصصی)	دکتر محمد صنیعی آباده	استادیار	

تقدیم به

پدر عزیز

و

مادر مهربانم

تشکر و قدردانی

الْحَمْدُ لِلّهِ الَّذِی هَدَانَا لِهَــذَا وَمَا کُنَّا لِنَهْتَدِیَ لَوْلا أَنْ هَدَانَا اللّهُ

سپاس خدای را که با یاری خویش بر من منت نهاد تا گامی دیگر در راه پیشرفت و اعتلای خود بردارم. امید آن که با بهره‌گیری مفید از آموخته ها و اندوخته های این دوره بتوانم شکرگزار بخش کوچکی از بیکرانِ الطافش باشم.

با تشکر و سپاسگزاری از زحمات بی وقفه استاد گرامی جناب آقای دکتر جلیلی که همواره در طول این دوره با توصیه های خود، مسیر را بر من هموار نموده و مرا به مقصد مطلوب رهنمون شدند، و با تشکر از آقای دکتر آبادی که از مشاوره های ایشان بهره‌مند گردیدم.

همچنین از آقای رحمانی‌منش نیز به دلیل راهنمایی‌های سودمند ایشان در انجام این پژوهش قدردانی می‌نمایم.

بخشی از این پژوهش با حمایت مالی مرکز تحقیقات مخابرات ایران تحت قرارداد شماره ۱۹۲۳۰/۵۰۰ به انجام رسیده است.

حجّت گهرگزی

آبان ماه ۱۳۹۱

چکیده

پروتکل OLSR به عنوان یکی از چهار پروتکل مسیریابی استاندارد برای شبکه های اقتضایی سیار، در برابر سوءرفتارهای انجام شده از جانب گره‌های مجاز شبکه آسیب‌پذیر است. سیستم‌های تشخیص نفوذ برای شناسایی این سوءرفتارها ارائه می‌شوند. سیستم تشخیص ناهنجاری نوعی از این سیستم هاست که سعی می‌کند رفتار غیر عادی را با یادگیری الگوی رفتار عادی شبکه شناسایی کند. یک مسئله مهم در مورد این سیستم ها مجموعه خصیصه هایی است که برای جمع آوری داده های مورد نیاز استفاده می‌نمایند. از آنجا که حمله‌های مختلف بر بخش‌های مختلف رفتار شبکه اثر می‌گذارند یک سیستم تشخیص ناهنجاری که از تعداد خصیصه‌های کم و نامناسب استفاده می‌کند قادر به تشخیص همه ناهنجاری‌ها نیست و از طرفی تعداد خصیصه‌های زیاد نیز ممکن است باعث کاهش دقت شود. به منظور ایجاد سیستم‌های تشخیص نفوذ در شبکه‌های اقتضایی که برای مسیریابی پروتکل OLSR را به کار می‌برند از دو رویکرد کلی استفاده می‌شود: تغییر و توسعه پروتکل، و روش های یادگیری ماشین. در این پژوهش ما مجموعه ای از خصیصه های پروتکل OLSR را برای پوشش تمام جنبه های رفتاری آن معرفی، و با استفاده از رویکرد یادگیری ماشین یک سیستم تشخیص ناهنجاری بر اساس جمع‌آوری مفهومی داده‌ها (CDC-ADS) ارائه می‌کنیم. این سیستم خصیصه ها را بر اساس منبع داده‌ها در چهار گروه در نظر گرفته و سپس یک الگو برای داده‌های عادی در هر گروه یادگیری می‌کند. برای تعیین عادی یا غیرعادی بودن یک رفتار، نظرات الگوهای یادگیری شده در رابطه با آن رفتار (شاخص‌های ناهنجاری) اخذ و تجمیع می‌گردند. ما برای تجمیع شاخص‌های ناهنجاری یک شیوه مبتنی بر انتخاب و میانگین‌گیری را معرفی می‌کنیم که بر طبق آن سه عدد از شاخص‌ها به عنوان خوش‌بین، بدبین، و علاقه مندی نمونه (شاخصی که نمونه مورد ارزیابی تمایل دارد با آن سنجیده شود) گزینش و از آن‌ها میانگین‌گیری می‌شود. آزمایشات نشان می‌دهد که جمع‌آوری داده ها در چهار گروه و ترکیب نظرات با شیوه مبتنی بر انتخاب و میانگین‌گیری، در مورد حمله‌های گوناگون نرح تشخیص را افزایش و نرخ هشدار نادرست را کاهش می‌دهد. همچنین ارزیابی‌ها با شرایط گوناگون شبکه‌ای (سرعت ها و بازه های زمانی مختلف) بیانگر قدرت و جایگاه CDC-ADS می‌باشد.

کلید واژه : شبکه اقتضایی سیار، پروتکل OLSR، تشخیص ناهنجاری، دسته بندی تک‌کلاسی، گروه متدها.

فهرست مطالب

عنوان **صفحه**

فهرست جدول‌ها

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فهرست اختصارات

علامت اختصاری	شرح
ADS	Anomaly Detection System
CARRADS	Cross layer based Adaptive Real-time Routing Attack Detection System
CDC-ADS	Conceptual Data Collection based Anomali Detection System
DoS	Denial of Service
IDS	Intrusion Detection System
MANET	Mobile Ad hoc Network
MDS	Misuse Detection System
MPR	Multi Point Relay
OCC	One-Class Classification
OLSR	Optimized Link State Routing
OPTI	Optimistic Index
PESI	Pessimistic Index
SFI	Sample Favorite Index
SOM	Self Organizing Map

فصل اول:

کلیات

۱-۱- پیشگفتار

شبکه های کامپیوتری از سال های آغازین پیدایش ریزکامپیوترها مورد توجه قرار گرفتند. با گسترش فناوری‌های مخابراتی، شبکه های بی سیم به وجود آمدند، در کنار شبکه های سیمی توسعه یافتند و همچنان در مجامع تحقیقاتی و حوزه کاربرد، جزء مباحث روز به شمار می‌روند.

شبکه های بی سیم از نظر شالوده و زیربنا به دو دسته باساختار[1] و اقتضایی[2] (بدون ساختار) تقسیم می‌شوند. شبکه های دارای ساختار توسط نقاط دسترسی به یک شبکه سیمی بزرگ متصل می‌گردند اما شبکه های اقتضایی، میزبان های بی‌سیمی هستند که به صورت خود سازمان یافته با یکدیگر ارتباط برقرار می‌کنند.

شبکه‌ی اقتضائی سیار[3]، یک مجموعه از گره‌های سیار بی‌سیم را شامل می‌شود که می‌توانند به صورت پویا و مستقل از شبکه‌های دیگر خود را در یک همبندی اختیاری و موقت سازمان دهی کنند و به این وسیله به افراد و ابزار اجازه دهند تا به طور مداوم در محدوده‌ای که هیچ زیرساخت از پیش تعیین شده‌ای وجود ندارد با هم ارتباط داشته باشند [۱].

گسترش و پیشرفت ابزارهای ارتباطی سیار از جمله تلفن سلولی و کامپیوترهای قابل حمل، انقلابی در جامعه اطلاعاتی بوجود آورده‌است، ابزارهایی که هر روز قوی تر و ارزان تر می‌شوند. ما در حال گذر از نسل کامپیوترهای شخصی به نسل کامپیوترهای همه جا حاضر هستیم. طبیعت این کامپیوترها این الزام را به وجود می‌آورد که شبکه ها به صورت بی سیم باشند، بنابراین زمینه شبکه های بی سیم در حال رشد نمایی است [۲]. شبکه‌های اقتضایی علاوه بر مسائل شبکه‌های بی‌سیم معمولی، با چالش های منحصر به فردی نیز رو به رو هستند، از جمله می‌توان به موارد زیر اشاره کرد [۲]:

- زیرساخت ثابتی در این شبکه‌ها وجود ندارد.

---

[1] Infrastructure
[2] Ad hoc
[3] Mobile Ad hoc Network (MANET)

- در این شبکه ها مسیریاب اختصاصی وجود ندارد.
- سرویس‌ها (یی مانند مدیریت شبکه) دراین شبکه‌ها باید توزیع شده باشند.
- کانال مورد استفاده از سیگنال‌های دیگر محافظت نمی شود.
- این شبکه‌ها قابلیت اطمینان بسیار پایینتری دارند.
- همبندی این شبکه‌ها پویا است.
- قدرت گره‌ها درحال تغییر و انرژی آنها محدود است.

۱-۲- مسیریابی در شبکه های اقتضایی

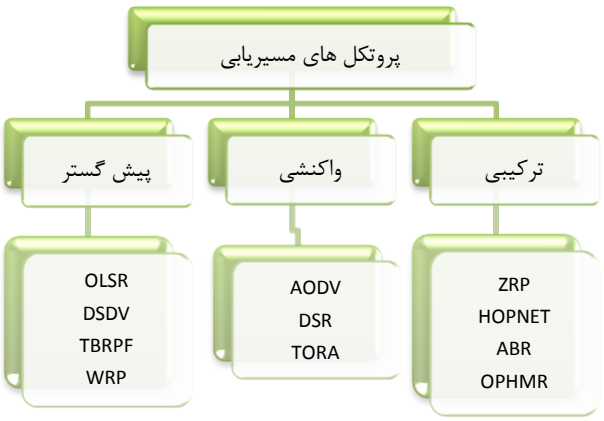
طبیعت پویای شبکه‌های بی‌سیم اقتضائی باعث می‌شود همبندی شبکه مکررا و به صورت غیرقابل پیش بینی تغییر کند، که این باعث پیچیدگی مسیریابی در میان گره‌های شبکه می‌شود. جنبه دیگر این پیچیدگی لزوم مشارکت تمام گره‌های شبکه در فرآیند مسیریابی است. بر این اساس پروتکل های متفاوتی به منظور مسیریابی معرفی شده اند که هر کدام سعی می‌کنند به نحوی این مسئله را حل نمایند.

.پروتکل های مسیریابی در شبکه‌های بی‌سیم اقتضائی به سه دسته: پیش‌گستر[1]، واکنشی[2] و ترکیبی تقسیم می‌شوند (شکل ۱-۱). پروتکل های پیش‌گستر تلاش می‌کنند تا اطلاعات مسیریابی را به روز نگه دارند. برای این کار، بسته به طراحی، هر گره اطلاعات به روز خود را بین همسایگان خود و یا در کل شبکه پخش می‌کند. زمان توزیع این اطلاعات می‌تواند به صورت دوره‌ای و یا برحسب وقوع رخداد درنظر گرفته شود. به بیان دیگر با استفاده از این پروتکل ها، هر گره در هر زمان مسیر به سایر گره‌ها را می‌داند. از آنجا که این پروتکل‌ها اطلاعات خود را در جدول نگهداری می‌کنند، به پروتکل‌های برمبنای جدول نیز معروف هستند. مهمترین پروتکل های پیش گستر عبارتند از: OLSR[3] و TBRPF[4] [۳].

پروتکل های واکنشی بر خلاف پروتکل‌های پیش‌گستر تنها زمانی بین دو گره مسیر ایجاد می‌کنند که بسته‌ای برای ارسال وجود داشته باشد. در این هنگام مبدأ از طریق فرایند کشف مسیر، مسیر مورد نظر را ایجاد می‌کند. این مسیر تا زمانی نگهداری می‌شود که دیگر بسته ای برای ارسال وجود نداشته

[1] Proactive
[2] Reactive
[3] Optimized Link State Routing (RFC3626)
[4] Topology dissemination Based on Reverse Path Forwarding (RFC 3684)

باشد، یا گره مقصد غیرقابل دسترس شود، و یا زمان استفاده از آن به پایان برسد. از مهمترین این پروتکل ها می‌توان AODV[1] و DSR[2] را نام برد [۳].



شکل ۱-۱: پروتکل های مسیریابی شبکه های اقتضایی

دسته سوم، ترکیبی از پروتکل های پیش گستر و واکنشی را مورد استفاده قرار می‌دهند به این صورت که مسیرهای موجود در بخش هایی از شبکه را به طور دائم نگهداری کرده و برای سایر بخش ها (معمولا فواصل دور) در هنگام نیاز مسیر را ایجاد می‌کنند. پروتکل های ZRP[3] و HOPNET نمونه هایی از این دسته می‌باشند [۳, ۴].

بعضی از خصوصیاتی که باید در طراحی پروتکل‌های مسیریابی مورد توجه قرار گیرد عبارتند از: منابع محدود، تعامل همبندی متغیر، مقیاس پذیری، پشتیبانی از ارتباطات یک‌طرفه، اطمینان، امنیت، و پشتیبانی از کیفیت سرویس [۲].

۱-۳- موضوع پژوهش

همچون هر سیستم کامپیوتری، یکی از مهم ترین مباحث شبکه های اقتضایی، مسئله امنیت است. با در نظر گرفتن ویژگی‌های منحصر به فرد این شبکه ها به ویژه در لایه شبکه، امنیت این لایه اهمیت بیشتری پیدا می‌کند.

ماهیت بی سیم بودن، تحرک داشتن، و فقدان ساختار اولیه و مسیریاب ثابت سبب شده‌است تا شبکه های اقتضایی ویژگی‌های منحصر به فردی داشته باشند که نمود واقعی آن ها در لایه شبکه و مسیریابی است. در این شبکه ها تمام گره‌ها باید علاوه بر انجام وظایف عادی خود، مانند مسیریاب عمل

[1] Ad hoc On demand Vector Distance (RFC 3561)
[2] Dynamic Source Routing (RFC 4728)
[3] Zone Routing Protocol

کرده و در فرآیند مسیریابی شرکت نمایند. از طرفی نکته قابل توجه در مورد پروتکل های مسیریابی این است که آن ها همه گره‌های شبکه را سالم و درستکار فرض می‌کنند، لذا هیچ گونه تمهیدات امنیتی[1] در آن ها در نظر گرفته نشده‌است. در نتیجه گره‌های بدخواه[2] می‌توانند به را حتی باعث ایجاد اختلال در کار شبکه و یا حتی فروپاشی کامل آن شوند.

سوء رفتار[3] در شبکه های اقتضایی از رفتارهای نادرست و ناخواسته گره‌ها و یا حملات، که می‌توانند از جانب گره(های) متخاصم خارجی و یا گره (های) بدخواه داخلی روی دهند، ناشی می‌شود. برای مقابله با سوءرفتارها به طور کلی دو رویکرد مورد توجه قرار گرفته‌است: ۱) افزودن بعضی مکانیزم های امنیتی مانند تصدیق اصالت[4] به پروتکل مسیریابی و ۲) ایجاد سیستم‌های تشخیص نفوذ[5]. سیستم‌های تشخیص نفوذ از دید روش تشخیص، در دو دسته تشخیص ناهنجاری (رفتار غیرعادی)[6] و تشخیص سوء استفاده[7] گروه بندی می‌شوند [۵].

سیستم‌های مبتنی بر تشخیص ناهنجاری، سعی می‌کنند تا با استفاده از روش های یادگیری، الگوهای رفتار عادی شبکه را ایجاد نمایند، از آن پس هرگونه رفتار مغایر با الگوهای شناخته شده، سوء رفتار تشخیص داده می‌شود. مزیت این رویکرد کشف حملاتی است که تاکنون ناشناخته بوده اند، اما معمولا نرخ هشدار نادرست[8] آن زیاد است. در مقابل، سیستم‌های تشخیص سوء استفاده، الگوی هر بدرفتاری خاص را شناسایی و یادگیری کرده و مواردی را که با آن تطابق داشته باشد به عنوان بدرفتاری یا حمله اعلام می‌کنند. این سیستم ها به نسبت سیستم‌های تشخیص ناهنجاری، نرخ هشدار نادرست پایینتری دارند، اما امکان تشخیص حملات نو و ناشناخته وجود ندارد [۵].

پروتکل مسیریابی OLSR به عنوان یکی از چهار پروتکل استاندارد ارائه شده برای شبکه های اقتضایی و مهمترین پروتکل پیش‌گستر، در حال حاضر در مجامع تحقیقاتی و همچنین کاربرد مورد توجه قرار گرفته‌است. دلایل این توجه را باید در تغییر ماهیت شبکه های اقتضایی از شبکه هایی با کاربرد نظامی به شبکه های عمومی تر مانند شبکه های ارتباطی تیم های امداد و نجات و یا حتی شبکه های سرگرمی جستجو کرد که محیط های بزرگ و متراکم، و نیازهای جدیدی مانند کیفیت سرویس[9] را مطالبه می‌کند.

---

[1] Security Measures
[2] Malicious
[3] Misbehavior
[4] Authentication
[5] Intrusion Detection System (IDS)
[6] Anomaly Detection System (ADS)
[7] Misuse Detection System (MDS)
[8] False Alarm Rate
[9] Quality of Service (QoS)